

3:23-MJ-2017

AFFIDAVIT

FILED

JAN 27 2023

I, Paul B Gilbride, being duly sworn, hereby depose and state that the following is true to the best of my information, knowledge, and belief:

Clerk, U. S. District Court
Eastern District of Tennessee
At Knoxville

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the U.S. Department of the Energy, Office of Inspector General (DOE-OIG), and have been since 2013. Between 2008 and 2013, I was a Special Agent with the United States Secret Service. During my law enforcement career, I have investigated financial fraud, network intrusions, child pornography, extortion, threats against protected persons, counterfeit currency, credit card fraud and other electronic crimes. I completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center (FLETC), and the United States Secret Service Special Agent Training Course (SATC), where I received specialized training concerning the execution of search warrants involving digital media and the proper handling of evidence. While acting in my official capacity, I am authorized to investigate violations of the laws of the United States. I am currently assigned to the DOE-OIG Cyber Investigations and Forensics Analysis section, where I have previously investigated and/or participated in investigations of network intrusions, intellectual property theft, mishandling of classified data, threats affecting interstate commerce, child exploitation and child pornography offenses, which included surveillance, executing search warrants, and reviewing digital evidence containing numerous examples of child pornography. I have completed the Department of Homeland Security, Basic Computer Evidence Recovery Training Program (BCERT) and Advanced Computer Evidence Recovery Training Program (ACERT), as well as various other training in the area of computer forensics, which included child pornography and child exploitation. I am a U.S. Department of Energy - Office of Inspector General, Internet Crimes

Against Children (ICAC) Affiliate Task Force member. As part of my duties, I investigate criminal violations relating to child exploitation and child pornography, including violations pertaining to the illegal production, distribution, receipt and possession of child pornography, in violation of Title 18, United States Code, Sections 2251, 2252, and 2252A. I have received training and instruction in the field of investigation of child pornography and have had the opportunity to participate in investigations relating to the sexual exploitation of children. As part of my training and experience, I have reviewed images containing child pornography in a variety of formats (such as digital still images and video images) and media (such as digital storage devices, the Internet, and printed images).

2. This affidavit is submitted in support of an application for a search warrant for computers and related equipment (more fully described in Attachment A), and the data located therein, there being probable cause to believe that located in the place described in Attachment A are items described in Attachment B, being evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(A)(5)(B).

3. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(A)(5)(B) are located in the place described in Attachment A.

4. The information contained within the affidavit is based on my training and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

RELEVANT STATUTES

5. This investigation concerns alleged violations of 18 U.S.C. Sections 2252 and 2252A, relating to material involving the sexual exploitation of minors.

6. 18 U.S.C. Sections 2252 and 2252A prohibit a person from knowingly possessing or accessing sexually explicit images (child pornography) with the intent to view them as well as transporting, receiving, distributing or possessing in interstate or foreign commerce, or by using any facility or means of interstate or foreign commerce, any visual depiction of minors engaging in sexually explicit conduct (child pornography).

DEFINITIONS

7. The following definitions apply to this Affidavit and Attachment B to this Affidavit.

8. “Child Pornography” includes the definition in 18 U.S.C. § 2256(8) (any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct).

9. “Visual depictions” includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

10. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

11. Hewlett Packard Elitebook 850 Serial Number 5CG6171F23, hereinafter and in Attachments A and B the “Device”, is owned and managed by the United States Department of Energy, Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee. ORNL has assigned the computer name “LAP-0102323” to the Device. The Device is assigned to employee Dennis McCroskey (McCroskey). The assigned user account on the Device is “3om”.

12. Your Affiant believes there is probable cause to believe that the Device is or contains evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Section 2252(A)(5)(B). The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

13. Therefore, while your Affiant might already have all necessary authority to examine the Device, your Affiant seeks this additional warrant out of an abundance of caution to be certain that an examination of the Device will comply with the Fourth Amendment and other applicable laws.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

14. Based on my training and experience, your Affiant knows about the following items, hereinafter and below and in the Attachments “Device.”

15. Based on my knowledge, training, and experience, your Affiant knows that computers and digital storage devices can store information for long periods of time. Similarly, things that have been searched for and viewed via the Internet are typically stored for some period of time on a device. This information can sometimes be recovered with forensic tools.

16. Based on my knowledge, training, and experience, examining data stored on computers and digital storage devices can uncover, among other things, evidence that reveals or suggests who possessed or used the computer or digital storage devices.

17. There is probable cause to believe that things that were once stored on the Device may still be stored there, for at least the following reasons:

A. Based on my knowledge, training, and experience, I know that digital files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a digital storage device or computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

B. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

C. Wholly apart from user-generated files, computer storage media including digital storage devices and computers’ internal hard drives can contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because

special software is typically required for that task. However, it is technically possible to delete this information.

D. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” Forensic review may also disclose when and by whom the Internet was used to conduct searches, view material, and communicate with others via the Internet.

18. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information on the Device that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of the use, who used the Device, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

A. Data on the storage medium can provide evidence of a file that was once on the storage media but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer or device was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created. This information can be recovered months or even years after they have been downloaded onto the storage medium, deleted, or viewed.

B. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

C. A person with appropriate familiarity with how a digital storage device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

D. The process of identifying the exact electronically stored information on storage media that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer or digital storage device and the application of knowledge about how a computer or digital storage device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

E. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

F. Your Affiant knows that when an individual uses an electronic device to aid in the commission of a crime, particularly crimes involving the sexual exploitation of children, the individual’s electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From

my training and experience, I believe that an electronic device used to commit a crime of this type may contain: Multiple images and videos of Child Sexual Abuse Material that have been received and sent through cellular phone peer to peer applications to include BitTorrent, WhatsApp. The cellular phone can contain Wi-Fi connection IP addresses, cellular geo locations, images and videos will include date/ time stamps, peer to peer applications will contain potential names of suspects and associates, files that are known to Internet Crimes Against Children (ICAC) investigations.

G. Your Affiant also knows that those who engage in criminal activity will attempt to conceal evidence of the activity by hiding files, by renaming the format, (such as saving a .pdf image file as a .doc document file) or by giving them deceptive names such that it is necessary to view the contents of each file to determine what it contains.

H. A single compact disk can store dozens of images and hundreds of pages of text. The size of the electronic storage media (commonly referred to as a hard drive) used in home computers has grown tremendously within the last several years. Thumb drives with a capacity of 32 gigabytes are not uncommon. Flash cards with a capacity of 32 gigabytes are not uncommon. Hard drives with the capacity of 500 gigabytes up to 3 terabytes are not uncommon. These drives can store thousands of images and videos at very high resolution. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with video capture capabilities, and save that image to storage in another country. Once this is done, there is no readily apparent evidence at the "scene of the crime". Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

19. *Need to review evidence over time and to maintain entirety of evidence.* Your Affiant recognizes the prudence requisite in reviewing and preserving in its original form only such records applicable to the violations of law described in this Affidavit and in Attachment B in order to prevent unnecessary invasion of privacy and overbroad searches. Your Affiant advises it would be impractical and infeasible for the Government to review the mirrored images of digital devices that are copied as a result of a search warrant issued pursuant to this Application during a single analysis. Your Affiant has learned through practical experience that various pieces of evidence retrieved from digital devices in investigations of this sort often have unknown probative value and linkage to other pieces of evidence in the investigation until they are considered within the fluid, active, and ongoing investigation of the whole as it develops. In other words, the weight of each individual piece of the data fluctuates based upon additional investigative measures undertaken, other documents under review and incorporation of evidence into a consolidated whole. Analysis is content-relational, and the importance of any associated data may grow whenever further analysis is performed. The full scope and meaning of the whole of the data is lost if each piece is observed individually, and not in sum. Due to the interrelation and correlation between pieces of an investigation as that investigation continues, looking at one piece of information may lose its full evidentiary value if it is related to another piece of information, yet its complement is not preserved along with the original. In the past, your Affiant has reviewed activity and data on digital devices pursuant to search warrants in the course of ongoing criminal investigations. Your affiant has learned from that experience, as well as other investigative efforts, that multiple reviews of the data at different times is necessary to understand the full value of the information contained therein, and to determine whether it is within the scope of the items sought in Attachment B. In order to obtain the full picture and

meaning of the data from the information sought in Attachments A and B of this application, the Government would need to maintain access to all of the resultant data, as the completeness and potential of probative value of the data must be assessed within the full scope of the investigation. As such, your Affiant respectfully requests the ability to maintain the whole of the data obtained as a result of the search warrant, and to maintain and to review the data in the control and custody of the Government and law enforcement at times deemed necessary during the investigation, rather than minimize the content to certain communications deemed important at one time. As with all evidence, the Government will maintain the evidence and mirror images of the evidence in its custody and control, without alteration, amendment, or access by persons unrelated to the investigation.

20. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, copying and reviewing the contents of the Device consistent with the warrant. The warrant I am applying for would authorize a later examination and perhaps repeated review of the Device or information from a copy of the Device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the Device to human inspection in order to determine whether it is evidence described by the warrant.

BACKGROUND ON OAK RIDGE NATIONAL LABORATORY NETWORKS

21. The Oak Ridge National Laboratory (ORNL) is a Federal research laboratory managed by the United States Department of Energy in Oak Ridge, Tennessee. The laboratory conducts Federally funded research and development in many scientific fields. The ORNL network contains data to include sensitive and Controlled Unclassified Information. ORNL

utilizes many systems and practices to ensure the security of the ORNL network. Examples of systems utilized are firewalls, secure user accounts assigned to employees, virus protection and scanning software, and network/device management software. Security practices are performed on the ORNL computers and networks assigned to ORNL employees.

22. Some ORNL Employees, depending on their positions are assigned electronics to include computers and the use of ORNL networks to do their job. Further the employee is provided a unique usernames to access the ORNL computers and networks. The user account requires two factor authentication to access a device. This requires the user to enter a password as well as utilize a smart card in their possession. Users are required to read and accept a user agreement upon every password change. The Acknowledgement states the following:

You are advised that there is no expectation of privacy of your activities on any system that is owned by, leased, or operated by UT-Battelle on behalf of the U.S. Department of Energy (DOE). The Company retains the right to monitor all activities on these systems, to access any computer files or electronic mail messages, and to disclose all or part of information gained to authorized individuals or investigative agencies, all without prior notice to, or consent from, any user, sender, or addressee. This access to information or a system by an authorized individual or investigative agency is in effect during the period of your access to information on a DOE computer and for a period of three years thereafter. Anyone using the systems acknowledges their consent to, and understanding of, these terms and conditions.

I have read the Password Rules and responsibilities and the Acknowledgement statement, and I acknowledge, understand and accept these terms and conditions.

The user must then select "I do not agree", or "I agree".

23. McCroskey, and ORNL employee with user account "3om" accepted the user agreement on November 9, 2022.

24. Every time a user logs into a computer managed by ORNL the user is presented with the following logon banner.

This is a Federal computer system and is the property of the United States Government. It is for authorized use only. Users (authorized or unauthorized) have no explicit or implicit expectation of privacy. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorized site, Department of Energy, and law enforcement personnel, as well as authorized officials of other agencies, both domestic and foreign. By using this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorized site or Department of Energy personnel. Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

INVESTIGATION

25. On January 18, 2023, ORNL Cyber Security Personnel received an automated alert from an internal virus protection system on the network. The alert was triggered by file "4.exe" which was identified as running on the Device while connected to the ORNL network. ORNL Cyber Security Personnel initiated a review into the alert to identify if the file was a current or continuing threat to the security of the ORNL network. During the review, ORNL Cyber Security Personnel identified several file names which were suggestive of Child Pornography. Many files with names suggestive of Child Pornography were located in a folder on the internal hard drive of the Device, under the user account "3om". Examples of the file names are "1.5 yr old rape.webm", "2yo anal GIF.gif", "3yo anal fucked.mp4", "3yo orgasm papaw.wmv", "3yo closeup anal.mp4", "3yo slow anal.mp4" and "5yo anal nice.mp4".

26. On January 19, 2023, ORNL notified the Department of Energy OIG of the incident.

27. Process event logs from the Device indicate file "2yo enjoys finger fucking.mp4" was accessed by user "3om" on January 18, 2023 at approximately 6:45 PM Eastern Standard

Time. The video was watched using VLC Media Player, a commonly used program to view video files. The file is located on the Device in the user folder for “3om” under a folder named “Saved Games”.

28. On January 19, 2023, ORNL Cyber Security Personnel used the network management software to pull the file “2yo enjoys finger fucking.mp4” from the Device automatically the next time it connected to the network. The file was successfully pulled by the system when the Device connected to the ORNL network.

29. On January 20, 2023, your affiant reviewed the file “2yo enjoys finger fucking.mp4”, recovered from the Device. The file is a video, 42 seconds in length. The video shows a nude female infant laying on her back. An adult hand is seen rubbing the vagina of the infant. The adult hand then inserts a thumb into the infant’s vagina.

**INDIVIDUALS WHO HAVE A SEXUAL INTEREST IN CHILDREN AND POSSESS,
RECEIVE AND/OR DISTRIBUTE CHILD PORNOGRAPHY**

30. Based on my previous training and experience related to investigations involving Child Pornography and the sexual abuse of children, I have learned that individuals who possess, receive, distribute or access with intent to view child pornography have a sexual interest in children and in images of children. Based upon my knowledge, experience, and training in child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in the receipt and collection of child pornography:

A. The majority of individuals who collect child pornography are persons who have a sexual attraction to children. They receive sexual gratification and satisfaction from sexual fantasies fueled by depictions of children that are sexual in nature.

B. The majority of individuals who collect child pornography collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children. Non-pornographic, seemingly innocuous images of minors are often found on media containing child pornography. Such images are useful in attempting to identify actual minors depicted in child pornography images found during the execution of a search warrant. In certain cases, such images may also assist in determining the origins of a particular child pornography image or series of images.

C. The majority of individuals who collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They almost always maintain their collections in the privacy and security of their homes, cars, garages, sheds, and other secure storage locations, such as in a digital or electronic format in a safe, secure, and private environment, including in cloud-based storage online or on their person.

D. The majority of individuals who collect child pornography often seek out like-minded individuals, either in person or on the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. This contact helps these individuals to rationalize and validate their deviant sexual interest and associated behavior. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant messaging, and other similar vehicles.


E. The majority of individuals who collect child pornography maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with children, as a way of understanding their own feelings toward children, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials because of the psychological support they provide.

F. The majority of individuals who collect child pornography often collect, read, copy or maintain names, addresses (including e-mail addresses), phone numbers, or lists of persons who have advertised or otherwise made known in publications and on the Internet that they have similar sexual interests. These contacts are maintained as a means of personal referral, exchange or commercial profit. These names may be maintained in the original medium from which they were derived, in telephone books or notebooks, on computer storage devices, or merely on scraps of paper.

CONCLUSION

31. Based on the investigation described above, probable cause exists to believe that inside the Device (described on Attachment A), will be found evidence, fruits, and instrumentalities of a violation of Title 18, United States Code, Section 2252(A)(5)(B) (described on Attachment B).

32. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items described in Attachment A for the items listed in Attachment B. I declare under penalty of perjury that the foregoing is true and correct to the best of my information, knowledge, and belief.



Paul B. Gilbride Special Agent
U.S. Department of Energy
Office of Inspector General

SUBSCRIBED and SWORN before me this 24th day of January 2023.



JILL E. MCCOOK
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

DESCRIPTION OF LOCATION TO BE SEARCHED

Hewlett-Packard Elitebook 850, serial number 5CG6171F23 (hereinafter and in Attachment B the “Device”) which is the property of the U.S. Department of Energy. The Device is currently assigned to ORNL employee Dennis McCroskey.

ATTACHMENT B

DESCRIPTION OF ITEMS TO BE SEIZED AND SEARCHED

For the Device listed and described in Attachment A, the following items, that constitute evidence of the commission of, contraband, the fruits of crime, or instrumentalities of violations of Title 18, United States Code, Section 2252(A)(5)(B) (hereinafter "Subject Offense"):

1. Images or visual depictions of child pornography;
2. Records and information containing child erotica, including texts, images and visual depictions of child erotica;
3. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to violations of the Subject Offense;
4. Any and all information, notes, documents, records, or correspondence, in any format or medium, pertaining to child pornography or sexual activity with or sexual interest in minors;
5. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning Internet activity reflecting a sexual interest in minors or child pornography;
6. Any and all information, notes, software, documents, records, or correspondence, in any form and medium pertaining to any minor who is, or appears to be, the subject of any visual depiction of child pornography, child erotica, sexual activity with other minors or adults, or of sexual interest, or that may be helpful in identifying any such minors;
7. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the Device or by other means for the purpose of committing violations of the Subject Offense;
8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible child pornography;
9. Any and all information, records, documents, invoices and materials, in any format or medium, that concern any accounts with an Internet Service Provider pertaining to violations of the Subject Offense;
10. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to violations of the Subject Offense;
11. Records of Internet activity, including Internet Protocol addresses, firewall logs, transactions with Internet hosting providers, co-located computer systems, cloud computing services, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses

pertaining to violations of the Subject Offense or that show who used, owned, possessed, or controlled the Device;

12. Any and all information, documents, records, photos, videos, or correspondence, in any format or medium, pertaining to use or ownership of the Device, or that aid in the identification of persons involved in violations of the Subject Offense;
13. Credit card information, bills, and payment records pertaining to violations of the Subject Offense;
14. Information about usernames or any online accounts or email addresses used to access or obtain images of child pornography;
15. Descriptions of time, date, locations, items, or events showing or tending to show the commission of, or connecting or tending to connect a person to violations of the Subject Offense;
16. Evidence of who used, owned, or controlled the Device to commit or facilitate the commission of the crimes described, or at the time the things described in this warrant were created, edited, or deleted, including photographs, videos, logs, call logs, phonebooks, address books, contacts, IP addresses, registry entries, configuration files, saved usernames and passwords, documents, calendars, browsing history, search terms, metadata, user profiles, e-mail, e-mail contacts, messages (text or voice), instant messaging logs, file structure and correspondence;
17. Evidence of software that may allow others to control the Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security provisions or software designed to detect malicious software or unauthorized use of the device, and evidence of the lack of such malicious software;
18. Evidence of the attachment to the Device of other storage devices or similar containers for electronic evidence;
19. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Device;
20. Evidence of how and when the Device were used or accessed to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
21. The telephone number, ESN number, serial number, and/or SIM card numbers of or contained in the Device;
22. Passwords, encryption keys, and other access devices that may be necessary to access the Device; and
23. Contextual information necessary to understand the evidence described in this attachment.

If the government identifies seized communications to/from an attorney, the investigative team will discontinue review until a filter team of one or more government attorneys and other government personnel, as needed, is established. The filter team will have no previous or future involvement in the investigation of this matter. The filter team will identify and segregate communications to/from attorneys, which may or may not be subject to attorney-client privilege. At no time will the filter team advise the investigative team of the substance of any of the communications to/from attorneys. The filter team then will provide all communications that do not involve an attorney to the investigative team, and the investigative team may resume its review. If the filter team believes that any of the communications to/from attorneys are not actually privileged (e.g., the communication includes a third party), and if the investigation is not covert, the filter team will first seek to obtain agreement from the appropriate defense counsel before providing these attorney communications to the investigative team. If consulting with defense counsel is not possible or does not produce an agreement, the filter team will obtain a court order before providing these attorney communications to the investigative team.

DEFINITIONS:

24. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).
25. "Child Pornography" is defined in 18 U.S.C. § 2256(8), which includes as any visual depiction of sexually explicit conduct involving the use of a minor; a digital image, computer image, or computer-generated image that is, or is indistinguishable from that of a minor engaged in sexually explicit conduct; or a visual depiction that has been created, adapted, or modified to appear than an identifiable minor is engaging in sexually explicit conduct.
26. "Visual depiction" includes prints, copies of visual images, developed and undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).
27. "Child Erotica" means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions; this also includes texts or discussions regarding minors engaged in sexual acts or conduct.